**HAWAII HEALTH SYSTEMS**
**C O R P O R A T I O N**
*Quality Healthcare For All*

# COMPLIANCE ALERT 12-21

## *"Texting, Tweeting, and Emails, Oh My!" Remember to Encrypt or Send via Secure Method if PHI is Included*

**Executive Summary:** All emails, texts, tweets, and messages sent electronically that include protected health information (PHI) must be sent using a secure method that encrypts the message to ensure confidentiality.

**Secure Solution required:** As HHSC implements EMR system throughout our facilities, it is imperative that employees and staff remember that sending any protected health information (PHI) electronically through email, texting, and/or tweets requires a "secure solution."

- *Use *Secure* for emails including PHI when sent to an address outside of HHSC.* Currently, HHSC subscribes to the ZIX system. By putting *Secure* on the "Subject Line," HHSC servers know to encrypt the email so that it is secure. Currently, sending PHI via a secure email method (such as our ZIX) system helps prevent HIPAA data breaches. Data breaches are serious compliance issues, require notification to the Federal Government, and result in costs for mitigation and possible government fines.

- *Do not use personal email accounts to send PHI via email.* Despite promulgating that their emails systems are secure (Gmail, AOL, Roadrunner, Hotmail, Yahoo, etc.), no HHSC business emails including PHI should be sent over these private, personal email systems.

- *Do not send any PHI using "texting" or "tweets".* Currently, HHSC does not have any system in place to secure messages sent via texts and tweets. No confidential, sensitive, or PHI should be sent using text messaging. Private devices should not be used to text or tweet any PHI.

- *Be careful when transferring, forwarding, and/or replying to electronic messages that contain PHI.* If *Secure* is included in the subject line the email will be encrypted even when replying or forwarding. HOWEVER, always check when replying or forwarded to make sure that all the information contained in the original email and the subsequent email string needs to be included. Remember—when allowed, HIPAA permits only "minimally necessary" PHI to be sent.

- *Delete Information when transferring information from a secure environment.* Any time information is transferred from a secure environment, delete as much sensitive, PHI, or personally identifiable information as possible, leaving only what is truly necessary to accomplish the task.

  **Eliminate/Remove Personal Information if Possible When:**
  - Exporting information from a secure system
  - Passing information between departments
  - Transferring information to vendors for processing
  - Providing information to law enforcement agencies or courts
  - Moving information to a portable device, for example to take home, or to take with you while travelling. It is required that any PHI on a portable device be encrypted. Unless you can ensure the device (lap top, phone, iPad, etc.) is encrypted, no PHI should be placed on that device.

**Conclusion:** More than 50% of the data breaches reported to the Department of Health and Human Services involve the loss or theft of unencrypted computing devices or storage media. To reduce risk of a data breach: (a) collect no more sensitive information than necessary, (b) securely destroy sensitive information when no longer needed, and (c) encrypt what you have.

If you have any questions about IT security, please call the HHSC Chief Information Security Officer at 808-733-4090. If you think you may have a data breach occurrence, please contact the Chief Compliance and Privacy Officer, your Regional Compliance Officer, your manager, and/or report to the HHSC Corporate Compliance Hotline at 877-733-4189 or https://hhsc.alertline.com